

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF PUERTO RICO

DISH NETWORK L.L.C, ECHOSTAR
TECHNOLOGIES L.L.C., and
NAGRASTAR LLC

Plaintiffs

v.

Edgardo Carrasquillo Reyes, a/k/a
"Edgardo Carrasquillo", "Ed Reyes",
"Frank Reyes", "BluebirdPR" and
"Bluebird" d/b/a Generation IKS,
www.caribbeansystems.galeon.com
and JOHN DOES 1-3

Defendant

Case No.:

**DECLARATION OF JERRY LEE GEE
IN SUPPORT OF PLAINTIFFS' *EX*
PARTE MOTIONS FOR TEMPORARY
RESTRAINING ORDER, CIVIL
SEIZURE/IMPOUNDMENT ORDER,
ORDER TO SHOW CAUSE, ORDER
TEMPORARILY SEALING CASE,
ORDER FOR ASSET FREEZE, AND
ORDER FOR ACCOUNTING**

Jerry Lee Gee declares and says:

1. My name is Jerry Lee Gee.
2. I am making this declaration in support of the Plaintiffs' Ex Parte Motions for Temporary Restraining Order, Civil Seizure/Impoundment Order, Order to Show Cause, Order Temporarily Sealing Case, Order for Asset freeze and Order for Accounting.
3. I make this declaration from my own personal knowledge. Additionally, employees and agents of the Plaintiffs have investigated the Defendant in this civil action and they have set forth their findings in their declarations, those declarations being:
 - a. The Declaration of Kevin Gedeon, an employee of the Plaintiff, EchoStar Technologies L.L.C.;
 - b. The Declaration of Gregory Duval, an employee of the Plaintiff, NagraStar LLC;
and
 - c. The Declaration of Gerald Plot, a private investigator.

The declarations of these individuals should be examined for details regarding the piracy activities of the Defendant. I find the opinions and statements of Mr. Gedeon and Mr.

Duval to be truthful and believable. I also find the allegations of the investigator to be to be truthful and believable. Accordingly, my statements set forth herein are also based upon the evidence derived from the Plaintiffs' investigation and from the expert analysis related to the investigation.

4. Through this declaration I will describe the Plaintiffs' satellite television system. Some of my declaration will cover areas also addressed by Mr. Gedeon and Mr. Duval in their declarations, but I make my declaration with a special emphasis on the encryption technology involved.
5. As set forth in more detail below, I will describe the relationship between the three Plaintiffs. Essentially, DISH Network L.L.C. (individually referred to as "DISH.") runs a satellite television business; EchoStar Technologies L.L.C. (individually referred to as "EchoStar") manufactures and distributes the hardware for the DISH system; NagraStar L.L.C. (individually referred to as "NagraStar") creates the encryption technology for the system. All of these elements can be described as being part of the DISH system.
6. When describing the DISH system I will sometimes collectively refer to DISH and EchoStar Technologies as "DISH" for ease of reference. These companies were, prior to a corporate restructuring on or around January 2008, related business undertakings under the same parent company. DISH and EchoStar continue to work cooperatively to effect the secure distribution of DISH Programming to DISH subscribers. DISH holds the necessary rights to sell subscriptions and distribute DISH Programming to its subscribers in the United States, including licenses from the copyright owners of DISH Programming, and delivers DISH Programming to its subscribers via satellite using an encrypted programming signal. As mentioned above, EchoStar is a technology supplier to DISH. It is the developer and manufacturer of DISH receivers and related technology (described

further below), which is used as part of the DISH security system (as defined below).

Personal Background

7. I am employed by the Plaintiff NagraStar L.L.C. (hereinafter "NagraStar") as the Director of Field Security and Investigations.
8. I have been working for NagraStar since January of 2001.
9. Before coming to NagraStar I was employed by Pinkerton Consulting and Investigations in Denver, Colorado for three years. I was a supervisor of investigations for Pinkerton, and I conducted investigations pertaining to due diligence, executive protection, corporate investigations, insurance fraud, surveillance, bond investigations, and software piracy investigations, among other things. I investigated several hundred cases dealing with piracy of computer software developed by Microsoft.
10. Prior to working as a supervisor for Pinkerton, I was the operations manager for Pinkerton security in Denver, Colorado.
11. I also am a veteran of the United States Marine Corps where I worked in the intelligence field.
12. My focus with NagraStar is obtaining technical intelligence and data primarily for the technical security of NagraStar customers including DISH and its related corporate entity, EchoStar Technologies; my primary focus with NagraStar is satellite piracy fraud against DISH, but I also do similar work for a Canadian satellite entity.
13. As part of my work I routinely get information by conducting internet research and by engaging in person-to-person intelligence gathering. I follow up on leads, and gather information off the internet, and I pursue information and coordinate leads. I also direct undercover investigations and assess the information gathered therein.

14. I have actively assisted both local and federal enforcement agencies within the United States of America and Canada. I have acted as an expert during criminal raids, searches and seizures.
15. I have been called to testify in satellite piracy trials for the government of the United States of America and Canada at the municipal/county, state/provincial and federal jurisdictions of both countries.
16. Through my position as a Director with NagraStar I have gained considerable knowledge of the DISH system and of the piracy of DISH's signals.

The DISH System

17. DISH has invested several billion U.S. dollars in its distribution and broadcasting system. All programming distributed by DISH is delivered to one or more broadcast centers in Wyoming, Arizona, and elsewhere, where it is digitized, compressed, and scrambled. The scrambled signals are then transmitted to multiple satellites located in geo-synchronous orbit above the Earth.
18. More than fourteen million household and commercial viewers of DISH Programming can obtain hundreds of channels of programming in digital video and CD-quality audio. DISH, together with its affiliates, employs over 25,000 people.
19. DISH purchases the distribution rights, including copyright licenses, for most of the DISH Programming it sells from program providers such as network affiliates, pay and specialty broadcasters, cable networks, motion picture distributors, sports leagues, event promoters, and other programming rights holders. DISH contracts and pays for the right to distribute DISH Programming to its subscribers, and holds rights to exhibit the DISH Programming to them.

20. The satellites that transmit DISH Programming have relatively fixed “footprints” (*i.e.*, a terrestrial territory within which the scrambled satellite broadcast signals can be received). The “footprints” of the satellites used by DISH cover the United States, parts of Canada, parts of Mexico, and several Caribbean nations and territories, including Puerto Rico. The satellites relay the scrambled signals back to Earth, where they can be received by DISH’s subscribers.
21. In order to view DISH Programming, a consumer must obtain certain satellite system hardware consisting primarily of: (1) a satellite dish, (2) an integrated receiver/decoder (also called a “receiver”, “IRD” or a “set-top box”), and (3) a DISH smartcard (“DISH smartcard”) (collectively, the “Receiving Equipment”). In certain newer receivers, the DISH smartcard microprocessor technology is built directly into the receiver and the receiver is “cardless”. For purposes of this declaration, this built-in technology is included in the term DISH smartcard.
22. Satellite dishes can be mounted on a rooftop, deck railing, or other structure at the subscriber’s home or business. The signal is received by the dish and transmitted by wire to the receiver. The receiver processes and descrambles the incoming signal using the credit-card sized DISH smartcard. The DISH smartcard is loaded into the receiver through a slot in the unit (except in “cardless” units where the microprocessor is built into the unit). DISH subsidizes the cost of the receiving equipment in anticipation of revenues that will be received from authorized subscribers to DISH Programming.
23. The DISH smartcard is essential to the operation of the receiving equipment; it communicates with the receiver to enable the descrambling of DISH Programming. The DISH software and the security software contained in the receiver are licensed from NagraStar, which regards it as a trade secret and strictly confidential information that it

would not disclose to any third party.

24. Without a subscription, DISH does not authorize access to its scrambled DISH Programming. DISH provides the DISH smartcards to its subscribers for use with receivers for the sole purpose of enabling authorized access to DISH Programming. DISH smartcards are the property of DISH and must be returned to DISH on request. Any modification of or tampering with DISH smartcards is prohibited by DISH. Moreover, the terms on which DISH smartcards are made available to consumers provide that they are strictly non-transferable.
25. DISH expressly prohibits subscribers from reverse-engineering, decompiling, disassembling, tampering, or the modification of any software or hardware that forms part of the DISH smartcards and DISH receivers. Subscribers to DISH are granted a license to use the software contained in the components of DISH receivers only in conjunction with their lawful operation and as authorized by DISH. They are also prohibited from copying, modifying, or transferring the software in the DISH receivers.

The DISH Security System

26. Because DISH generates revenues through sales of subscription packages and pay-per-view programming, and because its ability to attract and retain distribution rights for copyrighted programming is dependent upon preventing the unauthorized descrambling of its signals, all of DISH's video channels, except for some promotional offerings, are digitally encoded and scrambled to prevent unauthorized viewing.
27. Since NagraStar's ability to generate revenues is dependent upon the ability of its licensees to use NagraStar conditional access technology to restrict access to their services to authorized paying customers, NagraStar devotes substantial resources to the continuing

development and improvement of the NagraStar conditional access technology, the investigation of misuse or piracy of the NagraStar conditional access technology, and enforcing its rights against individuals engaging in such activities.

28. DISH uses a complex encryption system that is combined with a scrambler/encoder system to form its rights management and security system (the “DISH security system”), which is designed to, among other things, prevent DISH Programming from being viewed by unauthorized persons.
29. The DISH security system serves two interrelated functions: (1) subscriber rights management, which allows DISH to “turn on” or “turn off” programming that a customer has ordered, cancelled, or changed; and (2) scrambling, which prevents individuals or entities who have not ordered DISH Programming from viewing it.
30. NagraStar provides DISH with DISH smartcards that are programmed and serialized (*i.e.*, assigned unique electronic identification numbers). DISH then provides the DISH smartcards to receiver manufacturers, who include one DISH smartcard with each receiver (unless the receiver is “cardless”, in which case it is built into the receiver). Each DISH receiver also has a unique identification number.
31. Upon the first activation of a customer’s subscription, DISH sends a signal to the DISH smartcard in order to “pair” the DISH smartcard to the customer’s DISH receiver. The unique identification numbers of the DISH smartcard and the DISH receiver are maintained in DISH’s subscriber management system. This pairing operation, using the two unique identification numbers and their associated secret keys, is mandatory for the proper operation of the DISH security system. Before being “paired”, a DISH smartcard is not authorized by DISH to be used with any receiver, and after “pairing”, the DISH smartcard can only be used with that specific receiver and the receiver can only be used

with that specific DISH smartcard. In addition, in order to descramble DISH Programming, the identification numbers and secret keys must also be “paired” with other keys transmitted by DISH in its satellite signal data stream.

32. When a DISH receiver receives encrypted DISH satellite signals, it locates a special part of the satellite signal data stream known as the encrypted entitlement control message and sends that encrypted entitlement control message to the DISH smartcard in the DISH receiver. When a customer selects a DISH Programming channel for viewing, the DISH smartcard checks to determine whether that channel is part of that customer’s subscription and, if it is, decrypts the “control word” for that channel and provides it to the receiver. The receiver uses the control word to descramble the DISH Programming signal so the selected channel can be viewed by the subscriber. The control words are changed at regular intervals as part of the DISH security system.
33. The DISH smartcard, in conjunction with the DISH receiver, is programmed to handle secure telecommunications over telephone lines with respect to viewer purchases of pay-per-view movies or other events. These communications are essential to DISH’s billing, accounting, security, and customer service. To enable these telecommunications, DISH directs DISH subscribers to connect their receiver to a telephone line.
34. The DISH smartcard (including the equivalent technology built into newer DISH receivers) is, therefore, fundamental to the DISH security system in that it prevents unauthorized program viewing, while permitting authorized receivers used by DISH’s subscribers to descramble the signals and permit program viewing in accordance with the subscriber’s authorized subscription package and pay-per-view purchases.
35. The subscriber agreement between DISH and its residential customers (the “Residential Customer Agreement”) sets out the terms and conditions under which DISH provides

services and equipment to its residential customers. In order to protect its rights in DISH Programming and the DISH Security System, DISH includes the following provisions in its Residential Customer Agreement:

2(H) Private Home Viewing Only. DISH Network provides Services to you solely for viewing, use and enjoyment in your private home. You agree that no Services provided to you will be viewed in areas open to the public, commercial establishments or other residential locations. Services may not be rebroadcast or performed, and admission may not be charged for listening to or viewing any Services. If your Services are viewed in an area open to the public, a commercial establishment or another residential location, we may disconnect your Services and, in addition to all other applicable fees, you must pay us the difference between the price actually paid for Services and the full applicable rate for such Services, regardless of whether we have the right to distribute such Services in such other location.

4(C) Smart Cards. Receiver(s) are equipped with a conditional access card ("Smart Card") inserted into a slot or otherwise installed in such receiver...**Smart Cards remain the property of DISH Network at all times and must be returned to us upon our request. Smart Cards are not transferable.** Your Smart Card will only work in the DISH Network receiver to which it was assigned by DISH Network...

4(G) Proprietary Components and Software. DISH Network receivers and Smart Cards contain components and software that are proprietary to DISH Network and its licensors. You agree that you will not try to reverse-engineer, decompile or disassemble, nor will you tamper with or modify, any software or hardware contained within any receiver or Smart Card. Such actions are strictly prohibited and may result in the termination of this Agreement, disconnection of your Services and/or legal action.

4(H) Software License. You are licensed to use the software provided in your DISH Network receiver(s), as updated by DISH Network, its licensors and/or its suppliers from time to time, solely in executable code form, solely in conjunction with lawful operation of the DISH Network receiver(s) that you purchased or leased, and solely for the purposes permitted under this Agreement. You may not copy, modify or transfer any software provided in your DISH Network receiver(s), or any copy of such software, in whole or in part. You may not reverse-engineer, disassemble, decompile or translate such software, or otherwise attempt to derive its source code, except to the extent allowed under any applicable laws. You may not rent, lease, load, resell for profit or distribute any software provided in your DISH Network receiver(s), or any part thereof. Such software is licensed, not sold, to you for use only under the terms and conditions of this license, and DISH Network, its licensors and its suppliers reserve all rights not expressly granted to you. Except as stated above, this license does not grant to you any intellectual property rights in the software provided in your DISH Network receiver(s). Any attempt to transfer any of the rights, duties or

obligations of this license is null and void. If you breach any term or condition of this license, this license will automatically terminate.

8(A) Piracy. Receiving any portion of the Services without paying for them and/or any direct or indirect act or attempted act to engage or assist in any unauthorized interception or reception of any portion of the Services is a violation of various U.S. federal and state laws and of this Agreement. The penalties for violating such laws can include imprisonment and civil damage awards of up to \$110,000 per violation.

8(B) Physical Address/Change of Address. When setting up your DISH Network account, you must provide us with the physical address where your Equipment will be located and your Services will be provided. A post office box does not meet this requirement. You must give us immediate notice of any change of name, mailing address, telephone number, or physical address where your Equipment is located...

[Emphasis added]

Satellite Piracy Overview

36. In late 1998, rumors began to circulate that “hackers” were compromising the NagraStar conditional access technology and the DISH security system, so that they could receive and descramble DISH Programming without authorization from or payment to DISH. Subsequent investigations confirmed these rumors to be true. In this Declaration, I refer to persons who were engaged in or connected with businesses that were engaged in various aspects of satellite television piracy or who otherwise participated in the piracy community as “pirates”.
37. In the months and years that followed, various types of equipment, devices, software, programming code, modified satellite television smartcards, satellite television receivers, computer servers, and other technology (collectively, “piracy technology”) appeared on the market to “hack” or circumvent the DISH security system and the NagraStar conditional access technology.
38. Generally, there have been five stages of piracy activity:

- (a) First, pirates manufactured and sold “pirate boards” that operated in place of, or in conjunction with, DISH smartcards;
- (b) Second, pirates offered services to re-program the software on DISH smartcards with piracy software to permit the smartcards to steal DISH Programming, and services to “update” or “fix” the piracy software following the deployment of electronic countermeasures (“ECMs”) by the Plaintiffs that deactivated illegally-modified smartcards;
- (c) Third, pirates sold piracy devices that permitted consumers to re-program the software on DISH smartcards themselves, and made piracy software available on numerous websites, sometimes for a charge or membership fee;
- (d) Fourth, dealers began selling so-called “free-to-air” (“FTA”) receivers that were capable of being programmed with piracy software to steal DISH Programming (so-called traditional FTA receivers as described below), and piracy software was offered on numerous piracy websites and regularly “updated” or “fixed” following the deployment of ECMs by the Plaintiffs that deactivated illegally-modified FTA receivers; and
- (e) Fifth, dealers began selling FTA receivers capable of being connected to the internet (so-called internet-enabled FTA receivers as described below) that were capable of communicating with so-called Internet Key Sharing (“IKS”)/Control Word Sharing servers that provided the “keys” and control words, over the internet, necessary to steal DISH Programming.

DISH Smartcard Piracy

39. The first three stages of piracy described above involved the “hacking” and “emulation” of

DISH smartcards. DISH's anti-piracy strategy includes the periodic introduction of new generations of DISH smartcards containing updated security software. The main purpose of developing and introducing successive generations of DISH smartcards is to foil hackers and render obsolete existing piracy devices. Converting DISH customers to new generations of DISH smartcards and switching the satellite signal data stream so that it can only be received by the new DISH smartcards requires the Pirates to start over again in attacking the DISH smartcards. DISH and NagraStar have invested and continue to invest significant time and money in these enhancements.

40. For many years, Pirates developed, designed, provided and sold piracy software created solely for the purpose of "programming", "cracking", "flashing", "glitching", and "modifying" DISH smartcards, DISH Receivers, or piracy devices; "repairing", "patching", "fixing" or "updating" illegally-modified DISH smartcards, DISH Receivers, or piracy devices that had been disabled by ECMs transmitted by DISH to attack illegally-modified DISH smartcards; and "blocking" ECMs from attacking illegally-modified DISH smartcards.
41. This led to a "cat and mouse" game in which DISH and NagraStar continually enhanced the security features of DISH smartcards and the DISH Security System, and Pirates continually attempted to find ways to attack the security technology contained in them.
42. In 2008, DISH transitioned its subscribers to a new generation of DISH smartcard, known as the ROM 241¹, which contained updated security technology. The ROM 241 rendered the DISH satellite signal data stream "secure" from unauthorized descrambling (because the ROM 241 security technology had not been compromised by Pirates) and DISH

¹ Pirates often refer to the ROM 241, and other NagraStar smartcards of the same generation used worldwide, as "Nagra 3" or "N3". This is because these smartcards succeeded a prior generation of DISH smartcards that was known as "Nagra 2" or "N2" by Pirates.

Programming could no longer be descrambled using traditional piracy software and devices. However, piracy based on FTA receivers and IKS piracy (the fourth and fifth stages described above) continued to proliferate. In 2012, DISH introduced its latest generation of DISH smartcard known as the ROM 552, which is being provided with all newly manufactured and re-manufactured DISH Receivers.

43. Pirates sometimes refer to the use of modified DISH smartcards or piracy devices as “testing” (*i.e.*, implying that they are used for the purpose of “testing” the Receiving Equipment) and sometimes refer to themselves as “testers” and piracy as a “hobby”. DISH and NagraStar do not authorize anyone to modify, alter, reprogram or “test” DISH smartcards or DISH Receivers for any purpose whatsoever. Legitimate subscribers to DISH would have no reason to “test”, tamper with, alter, program, or re-program DISH smartcards or DISH Receivers. Rather, the sole purpose of such activities would be to circumvent the DISH Security System to steal DISH Programming.

The Use of Free-To-Air Receivers for Satellite Piracy
Traditional Free-To-Air Receivers

44. In 2003, Pirates developed a new way to steal DISH Programming by using FTA receivers programmed with piracy software. FTA receivers were originally designed to receive “free-to-air” satellite television signals, which are either not scrambled or scrambled but available free of charge. There are numerous “free-to-air” television channels available in Canada and the U.S., which offer specific ethnic, religious, business, music, information and advertisement programming. “Free-to-air” channels and FTA receivers have existed for many years, and are today manufactured and sold by several companies under various brand names including iLink, Freesat, Dreambox, Openbox, and SonicView.
45. FTA receivers are similar to the receivers used by DISH in that they are a set-top box,

approximately the size of a DVD player, which contain descrambling circuits and software that enables them to receive and decrypt programming. Some FTA receivers also contain a smartcard reader.

46. Because FTA receivers and their use are legal, in certain circumstances, in the United States, they are attractive to Pirates as a “legal” product with which to engage in piracy activities. This cloak of legitimacy presents challenges to DISH and NagraStar in their enforcement activities.
47. Initially, Pirates acquired FTA receivers from their manufacturers and loaded piracy software onto the circuit chips contained within them so as to mimic a DISH smartcard. This form of piracy was known as “Smart Card Emulation”. To combat Smart Card Emulation, NagraStar developed and deployed ECMs that served to either (1) change the keys used to descramble DISH Programming, or (2) create another layer of security that the piracy software cannot circumvent. Unfortunately, these ECMs were short-term solutions because the coders usually developed and released new software (sometimes called a “fix” or “update”) that gave the FTA receivers the capability of once again descrambling DISH Programming without authorization from or payment to DISH.
48. Subsequently, “coders” (*i.e.*, software programmers) gained access to a part of DISH’s encrypted data stream that contains the Decryption Keys and Control Words used to scramble and descramble DISH Programming. The coders embedded these Decryption Keys and Control Words in the piracy software, which, when loaded onto the FTA receiver, gave the FTA receiver the capability of descrambling DISH Programming without authorization from or payment to DISH.

Internet-Enabled FTA Receivers and IKS Piracy

49. In or about 2007, Pirates began selling certain brands of FTA receivers in North America that were capable of using piracy software to obtain the Control Words required to descramble DISH Programming directly from computer servers via the Internet (“Internet-Enabled FTA Receivers”). Legitimate FTA receivers do not require information to be downloaded from the Internet in order to receive FTA programming.
50. Once piracy software (sometimes referred to as “IKS piracy software”) is loaded onto Internet-Enabled FTA Receivers (sometimes referred to as “flashed Internet-Enabled FTA Receivers” or an “unauthorized receivers”), the Internet connection permits the “sharing” of Control Words through “Internet Key Sharing” or “IKS”. The Internet-Enabled FTA Receiver contacts a specific computer server over the Internet (the “IKS Server”), which provides the Control Words necessary to descramble DISH Programming.
51. IKS Servers use DISH smartcards activated on legitimate DISH subscription accounts, together with legitimate DISH Receivers, to decrypt the Decryption Keys and Control Words and share them with the IKS Server’s end-users through the internet, thereby permitting the end-users to descramble and view DISH Programming without purchasing a subscription.
52. There is no legitimate use for an IKS Server.
53. Pirates who operate IKS Servers typically sell subscriptions to DISH Programming to their customers (“IKS Subscriptions”) over the Internet. There are also piracy dealers who sell subscriptions to end-users where the dealer is not the actual pirate who is operating the IKS server; in essence these dealers obtain subscriptions on the “wholesale” level and sell them at the retail level. Generally, end-users who have purchased Internet-Enabled FTA Receivers purchase IKS Subscriptions, load IKS piracy software onto the Internet-Enabled

FTA Receivers, enter the IKS Subscription access code for the IKS Server, and then configure their Internet-Enabled FTA Receiver to connect to the IKS Server and receive Control Words required to descramble DISH Programming.

54. IKS Servers may have periods of time in which they stop working. Pirates sometimes refer to IKS as being “down” during these periods, while they take steps to restore the functionality of the IKS Servers. This volatility of IKS Servers is a result of a number of factors, including (1) ECMs that disable specific brands of IKS Servers at different points in time; and (2) specific issues experienced by the operators of individual IKS Servers. Thus, at any given point in time, certain IKS Servers may be operational while others may not be, and the status of IKS Servers can change on a regular basis. An IKS Server that goes “down” may be “fixed” and operational within a matter of hours or days.
55. Pirates have also devised a means of using DISH Receivers together with certain Piracy Technology to access IKS Servers. This Piracy Technology includes circuit boards known as AVR boards and modified wireless (sometimes known as “wi-fi”) routers used to access the Internet and the IKS Server, to obtain decrypted Control Words (“IKS Routers”). Using the decrypted Control Words, an IKS Router together with a DISH Receiver can descramble and view DISH Programming, in a manner similar to an Internet-Enabled FTA Receiver.
56. In essence, Internet-Enabled FTA Receivers, IKS Servers, IKS Routers and related Piracy Technology function in place of authorized DISH smartcards and DISH Receivers to provide end-users with the decrypted Control Words from IKS Servers to steal DISH Programming.
57. In order to communicate the Control Words to a large number of end-users of the IKS Server before the Control Words change (which occurs frequently to maintain the security

of DISH Programming), an IKS Server typically requires multiple subscribed and activated DISH smartcards. This is because each DISH smartcard decrypting Control Words for the IKS Server can only handle a limited number of Control Word requests at any given time. Moreover, ECMs transmitted by DISH and NagraStar periodically disable the DISH smartcards used in IKS Servers. For these reasons, Pirates who operate IKS Servers require access to additional DISH smartcards to replace those that have been disabled.

58. Pirates who operate IKS Servers are unlikely to activate DISH subscriptions in their own names. Instead, they obtain DISH smartcards activated by a number of different subscribers with different programming authorizations and accounts. As a result, when the Plaintiffs identify the DISH smartcards being used in IKS Servers, they can only trace them back to the subscribers who activated them rather than to the Pirates operating the IKS Servers. If fraudulent identities are used to activate the subscriptions, the identities of the Pirates who operate the IKS Servers are even more difficult to determine.
59. It is not necessary for end-users who access IKS Servers to know where the IKS Servers are physically located. To the contrary, the Pirates who operate IKS Servers typically conceal the physical location of the IKS Servers. IKS Servers are typically hidden in locations known only to the Pirates who operate them (and who require physical access in order to maintain them and replace the DISH smartcards that have been disabled by ECMs). In many cases, their locations are masked by using so-called "proxy" servers located in foreign countries that make it impossible for NagraStar or DISH to trace the locations of the IKS Servers. I have been involved in several investigations of IKS Servers in which the Internet Protocol ("IP") addresses of the IKS Servers have turned out to be "proxy" servers located offshore, but the IKS Servers themselves have been located in

North America, typically within easy access of the Pirates who operate them (and who require physical access in order to maintain them). In some cases, Pirates operating IKS Servers have told end-users that the IKS Servers are located offshore, where they cannot be seized by the Plaintiffs, but this is unlikely to be true because the IKS Servers, or at least a portion of the hardware supporting them, must be situated within the “footprint” where DISH Programming can be received (*i.e.*, within continental North America, or in the case of DISH also in the US Virgin Islands, Puerto Rico and Hawaii).

60. IKS Servers, IKS Routers, and the related Piracy Technology used to access them have posed, and continue to pose, serious threats to the business interests and revenues of the Plaintiffs, by undermining the integrity of the NagraStar Conditional Access System and the security and billing systems of the Plaintiffs. By engaging in IKS piracy, end-users are able to obtain all the information they need to descramble DISH Programming directly from IKS Servers to permit end-users to steal DISH Programming. The threats posed by IKS piracy are primarily because:

- a. by using legitimate DISH subscriptions, they circumvent the DISH Security System and the NagraStar Conditional Access System built into the DISH smartcard;
- b. Internet-Enabled FTA Receivers and IKS Routers supported by an IKS Server recover easily from ECMs because Pirates simply need to replace the affected DISH smartcards or DISH Receivers with new, legitimately subscribed, DISH smartcards and DISH Receivers. There is no need for Pirates or end-users to re-program the Internet-Enabled FTA Receivers and IKS Routers after an ECM because the Control Words continue to be transmitted as soon as the Pirates replace the equipment in the IKS Servers;

and

- c. since Internet-Enabled FTA Receivers and IKS Routers rely on an IKS Server which contains legitimately-subscribed DISH smartcards, they are able to descramble DISH Programming despite the transition to new generations of DISH smartcards with security enhancements that Pirates have not hacked.

- 61. In some cases, the Plaintiffs have been able to identify the DISH smartcards being used to support IKS Servers, and deploy ECMs to disable those DISH smartcards. However, the ECMs cannot stop or shut down these IKS Servers permanently. Instead, Pirates can simply replace the disabled DISH smartcards with newly activated DISH smartcards and install them in the IKS Servers so that end-users can resume stealing DISH Programming.
- 62. The use of IKS Servers: (1) permits an incalculable number of end-users to steal DISH Programming, and (2) makes it extremely difficult for the Plaintiffs to locate and disable IKS Servers and identify the Pirates who establish and operate them.

Public vs. Subscription-Based IKS Servers

- 63. IKS servers are either public or subscription-based. Public IKS servers are accessible via the internet to any end-user who has an internet-enabled FTA receiver programmed with compatible piracy software. End-users are not required to register with or provide payment to the operators of public IKS servers in order to obtain control words for DISH Programming. A public IKS server typically operates for a single brand, rather than multiple brands, of internet-enabled FTA receivers. The manufacturers of specific brands of internet-enabled FTA receivers also appear to be involved in operating or otherwise supporting the operation of public IKS servers for their brands of FTA receivers. Although

end-users do not pay for access to a public IKS server, they typically pay higher prices to purchase internet-enabled FTA receivers than they would for “traditional” FTA receivers.

64. Subscription-Based IKS Servers are only accessible to end-users who have subscribed to, or registered with, the pirate(s) operating the Subscription-Based IKS Server. Operators of Subscription-based IKS servers typically offer for sale subscriptions of varying duration to DISH Programming without authorization from or payment to DISH (“IKS Subscriptions”). IKS subscriptions can often be purchased via the internet. Upon registering with and/or providing payment to the operator of a subscription-based IKS server, end-users are able to download piracy software and configure their internet-enabled FTA receivers to connect to the subscription-based IKS server and receive control words required to descramble DISH Programming, thus becoming IKS subscribers. Subscription-based IKS servers may operate for a single brand or multiple brands of internet-enabled FTA receivers. As noted above they may also provide control words to DISH receivers that have been modified or programmed, or connected to piracy devices that permit them, to download control words from the IKS server.
65. NagraStar regularly purchases, arranges for the purchase of, or obtains subscriptions to various IKS Services. By analyzing the data stream from IKS Services, NagraStar can identify the DISH smartcards that are providing the control words to descramble particular channels of DISH Programming. By using the DISH customer databases, the Plaintiffs can then determine the unique identifying numbers of the DISH receivers that are paired with these DISH smartcards and the DISH subscription accounts on which they are activated.
66. After identifying the DISH smartcards being used for an IKS Service the Plaintiffs can also determine the DISH customer account information associated with the DISH smartcards by using their customer databases. This customer account information is

usually fictitious, however, for each customer account DISH maintains an account profile with the customer's name, service address, telephone number, contact information, subscription package selection, billing information, and DISH smartcards and receivers (including the unique identification numbers of the paired DISH smartcards and receivers).

67. NagraStar can trace the DISH smartcards being used to feed control words to particular IKS servers, as determined by data stream analysis, to determine where and when they were purchased. Occasionally, this purchase evidence can be used to identify the actual individual who purchased these devices that are engaged in IKS piracy; DISH contracts with retailers who sell EchoStar equipment (receivers and smartcards) and the DISH retailers keep records of their sales for DISH in the normal course of their business and their purchase records can be used to identify individuals who have purchased activated smartcards used in IKS piracy.

Piracy Forum Websites

68. Many Pirates operate or participate in piracy web sites that serve as a "forum" for the dissemination and exchange of information pertaining to Piracy Technology and satellite piracy generally ("Piracy Forum Web Sites"). Piracy Forum Web Sites typically:
- (a) provide information and instructions on Piracy Technology, including sources of supply, product information, and product reviews;
 - (b) provide piracy software files for download to their users, including files necessary to support FTA receiver piracy, IKS piracy, and, prior to the release of the ROM 241 which rendered DISH smartcards "secure", DISH smartcard piracy;
 - (c) provide discussion threads on topics of interest to the piracy community;

- (d) provide links to and advertisements for other piracy web sites that sell Piracy Technology and related services and provide piracy-related information; and generally serve as a “community” for the exchange of information designed to permit consumers to unlawfully receive DISH Programming, and to permit Pirates to communicate with one another on piracy developments

69. High profile Piracy Forum Web Sites can have thousands or even tens of thousands of members, subscribers, and users. Other Piracy Forum Web Sites are “private”, with membership on an “invitation only” basis.

Investigation of the Defendant Edgardo Carrasquillo

70. Employees and agents of the Plaintiffs investigated the Defendant in this civil action. The Plaintiffs also retained a private investigator to conduct an investigation of the Defendant. The declarations of Kevin Gedeon and Gerald Plot should be examined for the details regarding the piracy activities of the Defendant. My statements set forth below are in part based upon the evidence derived from the Plaintiffs’ investigation and from expert analysis related to the investigation.

71. Carrasquillo has effectuated the capturing of control words and the placement of those control words on IKS servers from at least 200 activated smartcards purchased by Carrasquillo. These activated smartcards are or were feeding control words to the IKS servers known as “Fish TV”, “I Link”, “Hillo1”, “Kanadian” and “Master Server”; additionally there are at least six (6) DISH accounts associated with Carrasquillo which are involved in the capturing of the control words. Presumably Carrasquillo is also using his captured control words in his own IKS service which he is selling under the name “Generation IKS” (see below).

72. Carrasquillo is selling and offering to sell IKS subscriptions through his service, "Generation IKS", IKS panel distributorships, IKS panel hardware and IKS end-user hardware, including pre-programmed IKS hardware and IKS end-user hardware created by modifying EchoStar hardware; Carrasquillo is undertaking these activities through his website www.caribbeansystems.galeon.com, through email communications, and in-person.
73. During the course of this investigation I directed our laboratories to analyze the hardware programmed with software obtained by a DISH dealer from the Defendant. Our laboratory confirmed that the receiver purchased from the Defendant was indeed an internet-enabled DISH receiver programmed (" flashed") with IKS piracy software such that the modified device could, if properly modified, decrypt DISH's signals without authorization when receiving key words from an IKS server. This receiver was found to be modified for the purpose of decrypting DISH's signals without authorization; however, it was done so in a manner that made the receiver inoperable. Attached hereto are true and correct copies of the reports from our laboratories as:
- a. **Exhibit A**, pertaining to the DISH receiver #R0086047246 purchased in October 2013;
 - b. **Exhibit B**, pertaining to the "AVR board" purchased in October 2013; and
 - c. **Exhibit C**, pertaining to the wireless router connected purchased in October 2013.
74. Based upon my knowledge and based upon the other declarations in this action I am of the opinion that the internet-enabled, unauthorized receivers flashed with IKS piracy software and the Piracy Technology which are sold and/or distributed by the Defendant are:
- a. Primarily of use in the unauthorized interception of DISH signals;
 - b. Designed or produced for the purpose of circumventing the Plaintiffs' digital

encryption, which is a technological measure used by the Plaintiffs to control access to the works protected by the copyright laws of the United States and that the internet-enabled, unauthorized receivers flashed with IKS piracy software:

- i. have only limited commercially significant purpose or use other than to circumvent DISH's encryption and conditional access, technological measures that effectively control access to copyrighted programming; or
- ii. were marketed by Defendant, or others acting in concert with Defendant, with Defendant's knowledge, for use in circumventing DISH's encryption, a technological measure that effectively controls access to copyrighted programming.

75. Based upon my knowledge and based upon the other declarations in this action I am of the opinion that the subscriptions to a private IKS server which are distributed by the Defendant and the subscriptions to the other services to which the Defendant is feeding control words are services:

- a. Designed or produced for the purpose of circumventing the Plaintiffs' digital encryption, which is a technological measure used by the Plaintiffs to control access to the works protected by the copyright laws of the United States and that subscriptions to a private IKS server:
 - i. have only limited commercially significant purpose or use other than to circumvent DISH's encryption and conditional access, technological measures that effectively control access to copyrighted programming; or
 - ii. were marketed by Defendant, or others acting in concert with Defendant, with Defendant's knowledge, for use in circumventing DISH's encryption, a technological measure that effectively controls access to copyrighted

programming.

76. Based upon my knowledge and based upon the other declarations in this action I am of the opinion that by participating in the operation of an IKS server(s), selling and offering to sell IKS end-user subscriptions, selling and offering to sell IKS panel distributorships, selling and offering to sell end-user IKS hardware; and selling internet enabled modified EchoStar receivers which have been preprogrammed with piracy software files for use in IKS piracy to the Defendant's customers and to the customers of the other IKS services he was feeding control words to, he was assisting them in the unauthorized decryption of DISH's signals.
77. The Defendant is running his piracy business for his own commercial gain. The Defendant also clearly knows that he is engaging in the above referenced activities to assist his purchasers and the customers of the other IKS services he was feeding control words to in obtaining DISH's signals without authorization and that the Defendant knew that what he was doing was illegal.

Damages and Irreparable Harm

78. It is impossible for the Plaintiffs, without obtaining access to the Defendant's business records, to calculate the actual losses the Plaintiffs have sustained and continue to sustain as a result of the Defendant's piracy dealer operations from the his residence and from the www.caribbeansystems.galeon.com website.
79. The evidence suggests that these losses would be substantial. Based upon its previous experience in cases involving satellite piracy, DISH estimates that it loses approximately \$70.00 to \$200.00 (U.S.) per month in subscription and pay-per-view fees for each piracy device in use. On an annual basis, the loss to DISH is approximately \$840.00 to \$2400.00

(U.S.) for each piracy device. These wide dollar ranges are due to the varying levels of programming offered by the various IKS Services and the numerous pay-per-view events available to the IKS end-users using these services. However, the Plaintiffs do not know, and are unable to presently ascertain, the number of customers who have purchased subscriptions to a private IKS server, downloaded IKS piracy software or purchased the internet-enabled, unauthorized receivers flashed with IKS piracy software from the Defendant's residence or website, and thus cannot calculate with any certainty their damages from lost subscription revenues.

80. Additionally, without obtaining the Defendant's records from the Defendant's computer(s) the Plaintiffs are unable to ascertain the numbers of subscriptions to a private IKS server, IKS piracy software files and the internet-enabled, unauthorized receivers flashed with IKS piracy software sold and/or distributed by the Defendant. Thus, they are unable to calculate the damages related to their sale subscriptions to a private IKS server, IKS piracy software files and the internet-enabled, unauthorized receivers flashed with IKS piracy software. The records of the sales should be on the computer(s) and/or on paper records at the his real property location at Los Reyes, off Carr 842, near Km 1 Hm 9, Caimito, San Juan, Puerto Rico.

81. The conduct of the Defendant has caused or contributed to and continues to cause or contribute to significant and irreparable harm to the Plaintiffs. It deprives DISH of subscription and pay-per-view revenues and other valuable consideration, it compromises the DISH security system and the NagraStar conditional access technology and it infringes on the Plaintiffs' trade secrets and confidential and proprietary information, and interferes with the Plaintiffs' contractual and prospective business relations.

82. In particular, the actions of the Defendant causes the Plaintiffs irreparable harm in that

they:

- (a) deprive DISH of a presently incalculable (as a result of the inability to ascertain, trace, or account for all unauthorized uses of DISH Programming) number of existing and prospective customers;
- (b) cause DISH a loss of revenues, proceeds, profits, and other benefits that are also incalculable, because it is difficult for DISH to trace, calculate, or prove:
 - (i) how many persons are receiving DISH Programming without authorization and for what periods of time they have done so;
 - (ii) how much and which type of DISH Programming and how much pay-per-view programming these persons are receiving without authorization; and
 - (iii) the actual value of the DISH Programming being received without authorization;
- (c) compromise the integrity of the DISH security system and NagraStar conditional access technology, which were developed with the investment of considerable time and expense, and in particular undermines the ability of DISH to restrict access to their paying customers within the territory of their copyright licenses for DISH Programming;
- (d) exploit for commercial gain the Plaintiffs' trade secrets and confidential information in the DISH security system and NagraStar conditional access technology;
- (e) jeopardize the goodwill associated with the Plaintiffs' names and reputations in the marketplace, which in turn results in continuous losses of revenue, proceeds, and future business opportunities, profits, and other benefits that are impossible to ascertain at this time; and

(f) threaten to damage or destroy the relationships which the Plaintiffs have developed over many years with their suppliers and customers, including their ability to retain distribution rights for copyrighted programming as a result of their inability to restrict distribution thereof.

83. If relevant evidence were destroyed by the Defendant the Plaintiffs would also suffer irreparable harm from the loss of evidence that is essential to proving their case against the Defendant and quantifying their damages.
84. The conduct of the Defendant causes significant and irreparable harm specifically to the Plaintiff DISH. It deprives DISH of subscription and pay-per-view revenues and other valuable consideration. It compromises DISH's security system, infringes on trade secrets and the confidentiality of its proprietary information, and interferes with DISH's contractual and prospective business relations.
85. The conduct of the Defendant causes significant and irreparable harm specifically to the Plaintiff EchoStar by depriving EchoStar of revenues derived from the sale and/or distribution of legitimate DISH hardware and software, by compromising EchoStar's proprietary information, and by interfering with EchoStar's contractual and prospective business relations.
86. The conduct of the Defendant causes significant and irreparable harm specifically to the Plaintiff NagraStar by depriving NagraStar of revenues derived from the sale of legitimate NagraStar smartcards to DISH, by compromising NagraStar's proprietary information, and by interfering with NagraStar's contractual and prospective business relations.
87. Because the total number of users of the pirate hardware, software and services sold and distributed by the Defendant is unknown, and the extent and type of programming viewed by these users is highly variable, it is very difficult for the Plaintiffs to calculate the actual

losses they have sustained and continue to sustain as a result of the Defendant's actions. Thus, the Plaintiffs have no adequate legal remedy other than the injunctive relief sought in the Plaintiffs motion to address the continuing violation of its rights, and bring an end to Defendant's illegal acts. It is also extremely crucial to obtain the records, especially the sales records of the Defendant directly from the Defendant's computer(s) located at his residence. The Pirate services and devices offered by the Defendant serve but one purpose: to facilitate the unauthorized descrambling of DISH's scrambled subscription programming signals, without restriction and free of charge, by persons who are not entitled to descramble them. By continuing their activities, the Defendant has caused and threatens to cause the Plaintiffs irreparable harm.

88. Additionally, as of this point in time the Defendant does not appear to own significant property; he may not be able to pay for the substantial damages he has caused the Plaintiffs. The Plaintiffs need an injunction against the Defendant such there can at least be the threat of contempt to stop him from engaging in his piracy activities.
89. Based upon the nature of Defendant's businesses, there is good reason to believe that the Defendant is technologically sophisticated. It is also clear that the Defendant's business is conducted using computers, which will contain files pertaining to devices and services for pirating DISH Programming, records (including the names and addresses of suppliers and customers), correspondence, and e-mail communications relating to the piracy of DISH Programming. All of these computer files can be accessed and readily deleted, purged, encrypted or electronically transferred to other locations outside the jurisdiction of this Court in minutes, if not in seconds. Much of this evidence which will be relevant to the present litigation cannot be obtained from any other source.
90. Similarly, piracy software files, the computer records, and even hardware inventory would

be easy for the Defendant or persons acting under his direction to remove or destroy such items in their possession in the event they were to receive notice of this litigation.

91. Based upon my experience with piracy cases I believe that there is a real and substantial risk that the Defendant, who is a telecommunications piracy dealer, is the type of defendant that will be likely to dispose of, conceal, or destroy potentially incriminating evidence upon being served with notice of the proceedings herein. Additionally, the fact that this Defendant utilizes aliases when conducting his piracy operation supports the contention that this *particular* Defendant would be likely to dispose of, conceal, or destroy potentially incriminating evidence upon being served with notice of the proceedings herein. The destruction of evidence would frustrate the Plaintiffs' ability to obtain a remedy for the Defendant's wrongdoing and frustrate the process of this Court. This has occurred recently in several other cases involving the piracy of DISH Programming in the United States and Canada. Examples of those cases and instances of spoliation are set forth below:

- a. NagraStar brought a lawsuit in Canada against Sky High Electronics, its owner Tomislav Robic, and other individuals and businesses for distributing piracy devices. DISH seized computers and other evidence pursuant to an Anton Piller Order – the equivalent to the *ex parte* seizure and impoundment order sought in this action. Mr. Robic later coordinated the break-in of the storage facility that housed the seized evidence and destroyed it.
- b. NagraStar sued Panarex, Inc. and other Defendant in the United States District Court for the Central District of California, Case No. 07-cv-05897, for distributing piracy devices. Panarex, after being served with the complaint and a preservation letter, destroyed emails and software files exchanged with the Korean manufacturer of the

piracy devices.

- c. NagraStar brought a lawsuit in Canada against Digital Store, its owner Ravindranauth Ramkissoon, and other Defendant for distributing piracy devices. When law enforcement and counsel attempted to seize evidence under an Anton Piller Order, Ramkissoon delayed entry to the premises and attempted to remove or destroy evidence, including several computer hard drives. Ramkissoon also used the delay to remove computers and other evidence from his personal residence.
 - d. NagraStar made a surprise visit to David Smith, operator of a piracy-related internet forum *www.f2atv.com*. Smith told NagraStar that if he was sued all incriminating evidence would be destroyed. NagraStar brought suit against Smith in the United States District Court for the Eastern District of Kentucky, Case No. 09-cv-00038, and was granted an *ex parte* seizure order. Shortly thereafter, it was discovered that following NagraStar's initial visit Smith had burned a computer hard drive containing evidence of his involvement in piracy.
 - e. NagraStar sued Munid and Ootra Ramkissoon in the United States District Court for the District of New Jersey, Case No. 09-cv-06135, for facilitating the theft of DISH Programming. The Ramkissoons have recently claimed that after the complaint was served their computer hard drives were "stolen" along with the numerous DISH receivers and smartcards at issue in the case.
92. I have also reviewed the declaration of Attorney Daniel Lefkowitz from the case of *CSC Holdings, Inc. v. Charles Carillo et al* 3:04 cv 1617 (JBA) (See McLaughlin Declaration **Exhibit A**) which sets forth a litany of situations that clearly evidence the fact that telecommunications pirates are precisely the type of Defendant who would move, hide or destroy evidence if given notice of a hearing. Based on my experience, the situations set

forth in Attorney Lefkowitz's declaration typify the type of actions telecommunications pirates will engage in.

93. Based upon my experience with piracy cases, it is my opinion that Plaintiffs will need an *ex parte* civil seizure order and the other relief we are seeking in this action.
94. Based upon my experience with piracy cases, I am also aware that numerous pirate websites post the PACER filings that are made in cases that relate to satellite or cable television. Therefore, these websites would inform their visitors about electronic filings even if the filings themselves were being done without notice to the Defendant (*ex parte*).
95. The Defendant in this action is precisely the type of defendant that would normally keep track of the PACER filings on cable and satellite cases. Accordingly, I believe that this Court should temporarily seal this case until we are able to execute a civil seizure order at the Defendant's residence.

Need for Asset Freeze and Accounting

96. It is clear that the Defendant is engaging in these piracy activities wilfully for his own commercial gain and profit.
97. Based upon my experience with piracy cases, it is my opinion that the Plaintiffs will need a freeze on the Defendant's assets. Otherwise the Defendant can utilize the assets to simply carry on piracy activities.
98. Also, Based upon my experience with piracy cases, it is my opinion that without an asset freeze the Defendant could remove or hide his assets that were derived from the profits from the piracy activities such that the Plaintiffs would be unable to attain these profits.
99. Based upon my experience with piracy cases, it is my opinion that the Plaintiffs will need an accounting so as to determine precisely what the Defendant's assets are and where they

are located.

I declare this 8th day of July, 2014 under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.



Jerry Lee Gee